Claims

1. A process for configuring, across the Internet, a digital certificate for a network device, the process comprising:

building a secret data encryption key into a network device when the network device is manufactured;

maintaining the secret key and a corresponding unique identifier of the network device in a database server accessible over the Internet;

sending, across the Internet from the network device to the database server, a two-part message wherein the first part contains the unique identifier, the IP address of the network device and a request for a digital certificate, and wherein the first part is encrypted using the built-in secret key, and wherein the second part of the message has at least some of the same information as the first part of the message, including the unique identifier, but is not encrypted;

determining, by the database server, the secret key from the database using the unique identifier received in the second part of the message;

decrypting, using the secret key from the database, the first part of the message;

comparing the information in the decrypted first part of the message with the information in the second part of the message;

comparing the IP address from which the message was received and the IP address specified in the message; and

sending a digital certificate to the network device if the information matches and the IP addresses match.

2. A process for configuring a digital certificate for a network device in a network environment, the process comprising:

embodying a secret key into the device;

storing, by an entity responsible for embodying the secret key, the secret key and a unique identification number of the device in a secure database accessible by the entity and a certificate authority;

receiving, by a certificate authority, a two-part message from the network device requesting a digital certificate wherein the first part of the message includes the unique identification number and the second part of the message is an encryption of the first part of the message encrypted with the secret key;

determining, by the certificate authority, the secret key from the database using the unique identification number;

decrypting, using the secret key from the database, the second part of the message;

comparing the decrypted message with the first part of the message; and

sending a digital certificate to the network device if the two parts match.

3. The process of claim 2 wherein the network device is a fax machine.

4. The process of claim 2 wherein the network device is a printer.

5. The process of claim 2 wherein the network device is a modem.

6. The process of claim 2 wherein the entity embodying the secret key and the certificate authority are a same entity.

7. The process of claim 2 wherein the entity embodying the secret key is a manufacturer of the network device, and wherein the secret key is embodied in the device when the device is manufactured.

8. A network device having a unique identification number, the network device comprising:

a secret key embodied in said network device when the network device is manufactured;

means for generating a two-part message requesting, from a digital authority, a digital certificate wherein the first part of the message includes the unique identification number and the second part of the message is an encryption of ᵗhe first part of the message using the secret key; and

means for receiving a digital certificate.

9. The network device of claim 8 wherein the network device is a printer.

10. The network device of claim 8 wherein the network device is a fax machine.

11. The network device of claim 8 wherein the network device is a modem.

12. A computer system having a database, the computer system comprising:

means for receiving a secret key and a corresponding unique identification number of a network device from an entity responsible for embodying the secret key into the network device;

means for storing the secret key and the corresponding unique identification number in the database;

means for receiving a two-part message from the network device requesting a digital certificate wherein a first part of the message includes the unique identification number and the second part of the message is an encryption of the first part of the message encrypted by the network device using the embodied secret key;

means for accessing the database to find the secret key associated with the unique identification number from the first part of the message;

means for decrypting the second part of the message using the secret key from the database;

means for comparing the decrypted second part of the message with the first part of the message; and

means for sending to the network device a digital certificate if the decrypted part of the message matches the first part of the message.

13. A computer program, on a computer-usable medium, comprising:

means for enabling receipt of a secret key and a corresponding unique identification number of a network device from an entity responsible for embodying the secret key into the network device;

means for causing the secret key and the corresponding unique identification number to be stored in a database;

means for enabling receipt of a two-part message from the network device requesting a digital certificate wherein a first part of the message includes the unique identification number and the second part of the message is an encryption of the first part of the message encrypted by the network device using the embodied secret key;

means for causing an access to the database to find the secret key associated with the unique identification number from the first part of the message;

means for causing a decryption of the second part of the message using the secret key from the database;

means for comparing the decrypted second part of the message with the first part of the message; and

means for causing a digital certificate to be sent to the network device if the decrypted part of the message matches the first part of the message.

14. A method executed in a computer system having a database, the method comprising:

receiving a secret key and a corresponding unique identification number of a network device from an entity responsible for embodying the secret key into the network device;

storing the secret key and the corresponding unique identification number in the database;

receiving a two-part message from the network device requesting a digital certificate wherein a first part of the message includes the unique identification number and the second part of the message is an encryption of the first part of the message encrypted by the network device using the embodied secret key;

accessing the database to find the secret key associated with the unique identification number from the first part of the message;

decrypting the second part of the message using the secret key from the database;

comparing the decrypted second part of the message with the first part of the message; and

sending to the network device a digital certificate if the decrypted part of the message matches the first part of the message.